BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 083 749 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
14.03.2001 Patentblatt 2001/11

(51) Int. Cl.[7]: **H04N 7/16**

(21) Anmeldenummer: **00116072.0**

(22) Anmeldetag: **27.07.2000**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **07.09.1999 DE 19943698**

(71) Anmelder: **Deutsche Telekom AG**
53113 Bonn (DE)

(72) Erfinder:
- **Althoff, Jürgen**
  48429 Rheine (DE)
- **Boehnke, Norbert**
  81825 München (DE)

(54) Verfahren und Vorrichtung zur selektiven Datenübermittlung über ein Rundfunkübertragungssystem

(57) Die bekannten Verfahren zur selektiven Datenübertragung über ein öffentliches Rundfunknetz sind mit variabel verschlüsselten Daten im Abonnementsystem durchführbar, wenn nur die Adressaten im Besitz eines aktuellen ihnen persönlich zugeordneten Schlüssels, z. B. einer befristet gültigen Chipkarte in Verbindung mit einer PIN sind. Ein für einen Zeitabschnitt fester geheimer Code beinhaltet die Gefahr unbefugter Benutzung. Außerdem ist jede Art von Zeitrahmen für den Beginn und die Beendigung eines Abonnements zu beliebiger Zeit sehr hinderlich.

Die Erfindung löst dieses Zeitproblem mittels eines Systems mit mehreren Schlüsseln, von denen sich einer von Anwendung zu Anwendung verändert. Die abonnierten Daten kennzeichnet ein statischer anwendungsspezifischer Schlüssel (Longkey), die Abonnenten kennzeichnet ein erstes binäres statisches Schlüsselwort (Privatekey), aus denen vom Inhaltsanbieter ein dem Teilnehmer zugeordnetes zweites variables Schlüsselwort (Shortkey), und bei deren Aufbereitung ein aus diesen Schlüsseln errechneter dritter, immer variierender Schlüssel (Superkey) hinzugefügt wird.

Anwendungsgebiete der Erfindung sind alle Arten von gesicherter Datendistribution von einem Inhaltsanbieter über einen oder mehrere Sender an viele Empfänger

EP 1 083 749 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren der im Oberbegriff des Patentanspruch 1 und eine Vorrichtung der im Oberbegriff des Patentanspruchs 5 näher bezeichneten Art. Derartige Verfahren und Vorrichtungen sind allgemein bekannt und verbreitet und werden z. B. von kommerziellen TV- Anbietern für Antennen- und Satellitenrundfunk und Kabelfernsehen, auch für Pay- TV, für Sendungen benutzt, die nur mit Decoder empfangen werden können.

[0002] Sowohl öffentliche, als auch solche codierte Sendungen können zusätzlich mit Videotext versehen sein, der weitere Informationen enthält und mittels Videotext- Decoder empfangen wird, der auch für schnelleren Zugriff mit Grafik- Prozessor versehen sein kann, wie z. B. aus Langenkamp/Löwy „Megatext- IC für Videotext und Grafik" RFE 1994, Heft 7, Seiten 18 - 20 bekannt.

[0003] Aus DE 40 33 126 A1 sind auch Videotextsysteme bekannt, die Daten unter Verwendung einer Telefonleitung als Übertragungsmedium übertragen. Bei diesen Systemen werden Daten von Informationsanbietern in einem Informationszentrum akkumuliert und die akkumulierte Information wird Benutzern bzw. Teilnehmern zugeleitet, wenn sie diese über ihr Terminal anfordern. Es ist neben einem direkten auch an ein baumartiges Abrufverfahren gedacht. Während das Informationszentrum abgerufene Informationen übermittelt, ist eine Rückinformation über die beim Teilnehmer eingegangenen Bilder vorgesehen, die, nach einem Ausfall der Verbindung, bei neuerlichem Abruf mit einer Wiederherstellungstaste einen Anschluß an die bereits gesendeten Bilder gewährleisten soll. Die damit erreichbare Verminderung von Wiederholzeiten ist bei der notwendigerweise wegen der geringen Bandbreite langsamen drahtgebundenen Übermittlung ebenso wesentlich, wie beim „blättern" bei der Videotext-Übertragung über ein Fernseh-Empfangsgerät, das erheblichen Zeitaufwand des Teilnehmers und Zeitverzögerungen bis zur gewünschten Information verursacht. Auch fehlen bei solchen Geräten Archiv- oder Speichermöglichkeiten.

[0004] Diese Nachteile lassen sich verringern, wenn ein Computer mit einer Empfangseinrichtung unter Benutzung einer TV-Zusatzkarte mit Antennenanschluß und moderner Software als Wiedergabemedium benutzt wird. Diese kann auch Empfangskanal- Speicher enthalten und für Videotext und Datenrundfunk verwendbar sein.

[0005] Es sind auch andere Übertragungs-Systeme bekannt, die Daten in einem anderen Format als Videotext in den Prüfzeilen übertragen, z.B. INTERCAST von INTEL, das im Probebetrieb beim ZDF verwendet wird.

[0006] Mit solchen Mitteln sind auch selektive Datenübertragungen über ein öffentliches Rundfunkübertragungssystem bzw. über INTERNET mit verschlüsselten Daten im Abonnementsystem durchführbar, die nur von solchen Adressaten entschlüsselt werden können, die im Besitz eines aktuellen ihnen persönlich zugeordneten Schlüssels sind. Ein solcher Schlüssel kann, wie üblich, als befristet gültige Chipkarte in Verbindung mit einer PIN ausgeführt und evtl. codiert derart gespeichert sein, daß er nur dem Inhaltsanbieter mittels dessen geheimen Code die Identität des Adressaten verrät.

[0007] Die Verwendung eines solchen für einen Zeitabschnitt festen geheimen Codes stellt jedoch eine Gefahr sowohl für den Inhaltsanbieter als auch für den Adressaten dar, da mit dessen unbefugter Benutzung die Systemsicherheit zentral angegriffen werden kann. Außerdem ist jede Art von Zeitrahmen für den Beginn und die Beendigung eines Abonnements zu beliebiger Zeit sehr hinderlich. Es ist deshalb die Aufgabe der Erfindung, einen geheimen festen Schlüssel zu vermeiden und das Verfahren und die Vorrichtung so zu gestalten, daß ein Abonnement zu jeder beliebigen Zeit begonnen und beendet werden kann.

[0008] Die Erfindung löst diese Aufgabe mit den im Kennzeichen des Patentanspruchs 1 aufgeführten Verfahrensschritten.

[0009] Eine Vorrichtung, die zur Lösung dieser Aufgabe geeignet ist, ist im Kennzeichen des Patentanspruchs 5 beschrieben.

[0010] Vorteilhafte Aus- bzw. Weiterbildungen des Verfahrens sind in den Unteransprüchen 2 bis 4 beschrieben.

[0011] Eine vorteilhafte Weiterbildung der Vorrichtung beschreibt das Kennzeichen des Unteranspruchs 6.

[0012] Nachfolgend wird die Erfindung in einem Ausführungsbeispiel anhand der zugehörigen Zeichnungen näher beschrieben. Hierin zeigen die

- Fig. 1 eine Übersicht der Daten- Schlüsselfunktionen zum Anlegen einer Liste für den bedingten Zugang beim Inhaltsanbieter
- Fig. 2 eine Übersicht der Daten- Schlüsselfunktionen beim Versorgen eines Abonnement-Teilnehmers mit Daten und
- Fig. 3 eine Übersicht über die verwendeten Schlüssel

[0013] Die Figuren zeigen die Zusammensetzung der Daten und Schlüssel anschaulich und bedürfen keiner zusätzlichen Erklärungen. Es wird deshalb nachfolgend das Entstehen und Beenden eines Abonnements näher erklärt:

[0014] Vom Inhaltsanbieter wird eine Liste aller angebotenen Abonnements mit den zugehörigen Gebühren erstellt.

[0015] Der Kunde erhält ein Produktpaket mit einer Steckkarte für den Empfang der Datenpakete, Antennenanschluß, sowie aufgezeichnete Installationssoftware. Die im Produktpaket enthaltene Software führt

einen Sendersuchlauf durch und speichert die gefundenen Kanäle. Er kann auch durch die mitgelieferte Software auch bei der Anmeldung unterstützt werden.

[0016] Entschließt sich ein Kunde, ein Abonnement zu beantragen, so wird ihm zunächst unverschlüsselt eine Liste der angebotenen Abonnements mit den aktuellen Gebühren angezeigt.

[0017] Der Kunde wählt nun aus der Liste ein oder mehrere Abonnements, die er beantragen möchte, und füllt für die Anmeldung ein Formular aus.
Darin gibt der Kunde die notwendigen Informationen zu seiner Person ein, wie

- Name
- Straße
- Wohnort
- Zahlungsart
- gegebenenfalls Bankverbindung

[0018] Das ausgefüllte Formular kann der Kunde dann per Post, als Email oder als Fax an den Inhaltsanbieter senden.

[0019] Geht beim Inhaltsanbieter ein Abonnementantrag ein, so wird für jedes Abonnement auf der Grundlage der Kundeninformationen ein Paßwort (Privatekey) generiert. Dieses Paßwort wird zusammen mit der entsprechenden Gruppenbezeichnung, z.B.:

> Gruppe = TVToday, Paßwort(Privatekey) = 123456789abcd an den Kunden zurückgeschickt.

[0020] Nach Erhalt gibt der Kunde das Paßwort einmalig bei der entsprechenden Gruppenbezeichnung in ein dafür vorgesehenes Formular ein. Diese Daten werden gespeichert, und der Kunde ist damit für den Empfang von Daten der entsprechenden Gruppe freigeschaltet. Er erhält in einer Art Briefkasten, auf den er über die Taskleiste Zugriff hat, Informationen über die vorgesehenen Übertragungszeiten, zu denen der Computer dann eingeschaltet sein soll. Dieser kann während der Übertragung auch anderweitig benutzt werden, da die Daten direkt der Festplatte zum Speichern zugeführt werden.

[0021] Beim Empfang der Daten werden zunächst mögliche Empfangsfehler durch Wiederherstellung der Bitreihenfolge (Interleave) und durch einen Selbstkorrektur- Algorithmus korrigiert. Danach erfolgt mit Hilfe des gespeicherten Paßwortes (Privatekey) eine automatische Dekodierung der Daten.

[0022] Nach anschließender Dekomprimierung werden die Daten auf der Festplatte gespeichert und stehen zur Ansicht zur Verfügung.

[0023] Geht ein Abonnementantrag ein, so wird mit Hilfe eines Paßwortgenerators aus den persönlichen Daten des Kunden ein individuelles Kundenpaßwort (Privatekey) erzeugt, das an den Kunden zurückgeschickt wird. Mit Erhalt und Eintrag des Privatekey in die Software ist der Benutzer empfangsberechtigt.

[0024] Der Privatekey, den der Benutzer vom Inhaltsanbieter erhält, wird aus den persönlichen Daten (Name und Anschrift) des Benutzers berechnet. Außerdem läßt sich der Indexwert der Shortkey- Liste (Freigabefile) aus dem Privatekey berechnen.

[0025] Jedes Datenpaket wird vor der Sendung verschlüsselt (Superkey). Zu jedem verschlüsselten Datenpaket wird ein zusätzliches File (Freigabefile) erzeugt, das zur Entschlüsselung notwendige Informationen enthält. Das Freigabefile wird nur von den Kunden empfangen, die für die entsprechende Gruppe freigeschaltet sind. Durch eine Änderung des Freigabefiles nimmt die übrige Datenmenge durch die Verschlüsselung nicht zu.

[0026] Das fertige Datenpaket, welches das zugehörige Freigabefile beinhaltet, wird vom Inhaltsanbieter an den TV-Sender geschickt. Dort können die Daten dann zu den vorgegebenen Zeiten gesendet werden. Vor der eigentlichen Datensendung wird eine Zeigerseite mit der Information über den Sendetermin gesendet.

[0027] Verliert der Benutzer seine Empfangsberechtigung, z.B. wegen ausbleibender Zahlung der Gebühren, wird für ihn ein ungültiger Shortkey generiert. Mit diesem ungültigen Shortkey, den die Software des Kunden aus der Shortkey- Liste extrahiert, ist der Benutzer nicht mehr in der Lage, einen gültigen Superkey zu bilden, wodurch eine Dekodierung der empfangenen Daten unmöglich ist.

[0028] Wird ein Abonnement endgültig aufgelöst, so kann die entsprechende Indexposition in der Shortkey- Liste neu vergeben werden.

[0029] Mit dem beschriebenen Verfahren gelingt eine gesicherte Datendistribution von einem Sender an viele Empfänger mit den Eigenschaften:

- Adressierung beliebig vieler Benutzer bzw. Benutzergruppen
- Zeitlich variable Gültigkeit der Adressierung,
- Vermeidung hardwaregestützter Identifikation,
- Variabler Verschlüsselungsgrad,
- Schlüsselwechsel ist für jede Sendung möglich,
- Skalierbarer Verschlüsselungsgrad für jede Sendung.

Auflistung der verwendeten Schlüssel

Superkey

[0030] Die eigentliche Datensendung ist mit einem Superkey verschlüsselt. Ohne aktuellen Superkey ist kein Zugriff auf die Daten möglich. Der Superkey wird aus dem Longkey und dem Shortkey errechnet.

Longkey

[0031] Der Longkey ist der statische Teil des Superkeys. Für jede Gruppe wird einmalig ein Longkey bestimmt. Der Longkey wird mit der Zeigerseite gesen-

det.

Shortkey

[0032] Von der Zentrale wird für jeden Benutzer ein Shortkey generiert und daraus eine indizierte Liste erstellt. Diese Liste (Freigabefile) wird vor der eigentlichen Datensendung ausgestrahlt. Welcher Shortkey für welchen Benutzer bestimmt ist, wird durch den Index festgelegt. Dieser kann aus dem Privatekey des Kunden berechnet werden.

[0033] Nach seiner Anmeldung erhält der Benutzer vom Anbieter den Privatekey.

Der Privatekey wird aus den persönlichen Daten (Name und Anschrift) des Benutzers berechnet. Außerdem läßt sich der Indexwert der Shortkey- Liste (Freigabefile) aus dem Privatekey berechnen.

Patentansprüche

1. Verfahren zur selektiven Datenübermittlung über ein Rundfunkübertragungssystem, bei dem die Daten, die über dieses verteilt werden, mit vom Inhaltsanbieter verschlüsselten Zusatzdaten versehen werden, welche nur von solchen Adressaten entschlüsselt werden können, die im Besitz eines aktuellen, ihnen persönlich zugeordneten Schlüssels sind, **dadurch gekennzeichnet,** daß

   - den Daten statische anwendungsspezifische Schlüssel (Longkey), die den Inhalt kennzeichnen, , Sendezeit und Adressinformationen, und getrennt in einem Teilnehmerverwaltungssystem verschlüsselte Paßworte für Zugriffsberechtigungen zugeordnet werden,
   - vom Teilnehmerverwaltungssystem aus personenbezogenen Teilnehmerdaten ein erstes binäres statisches Schlüsselwort (Privatekey) gebildet wird,
   - aus dem vom Inhaltsanbieter mittels einer verschlüsselt gesendeten Zuordnungsliste ein dem Teilnehmer zugeordnetes zweites variables Schlüsselwort (Shortkey) nach Dekodierung der Zuordnungsliste mittels des Privatekey für die Bildung des Berechtigungsschlüssels entnommen und den Daten, die einen anwendungsspezifischen Schlüssel enthalten, bei deren Aufbereitung ein aus diesen Schlüsseln errechneter dritter variabler Schlüssel (Superkey) hinzugefügt wird, und daß
   - empfangsseitig alle eingegangenen Daten adresselektiv aufgenommen, mittels der personenbezogenen Teilnehmerdaten und des extrahierten Superkey auf Zugriffsberechtigung geprüft, und erst danach entschlüsselt, korrigiert und gespeichert werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Daten parallel zum Videotext vom Fernsehsender übertragen werden.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß vom Inhaltsanbieter zusätzlich unverschlüsselt eine Liste der jeweils angebotenen Abonnements mit zugehörigen Bestellbedingungen übertragen wird.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Inhaltsanbieter für das Beenden eines Abonnements einen ungültigen Shortkey generiert und diesen aus seiner Liste der Zugriffsberechtigten extrahiert.

5. Vorrichtung zur selektiven Datenübermittlung über ein Rundfunkübertragungssystem, bei der ein Inhaltsanbieter Datenpakete an die Sender liefert und beim Empfänger ein Computer mit einer Empfangseinrichtung für Datenrundfunk und mit einem Empfangskanal- Speicher ausgerüstet, und mit einem Antennenanschluß versehen ist,
   dadurch gekennzeichnet, daß die ausgesendeten Datenpakete, die vom Inhaltsanbieter an den Rundfunksender gehen, mit Adressen, Inhaltsgruppen-Bezeichnung und Sendezeit versehen, komprimiert, verschlüsselt und einem File zur Entschlüsselung versehen sind und daß die Empfangseinrichtung außer mit dem Empfangskanal- Speicher auch mit Abonnements- und Paßwort-Speichern und Filtern ausgerüstet ist und mit einen Schalter für die Verbindung zu einem dem Abonnement zugeordneten Bereich der Festplatte versehen ist.

6. Vorrichtung nach Anspruch 5, dadurch gekennzeichnet, daß die Empfangskanal- Speicher von den ausgesendeten Datenpaketen fernsteuerbar gestaltet sind.

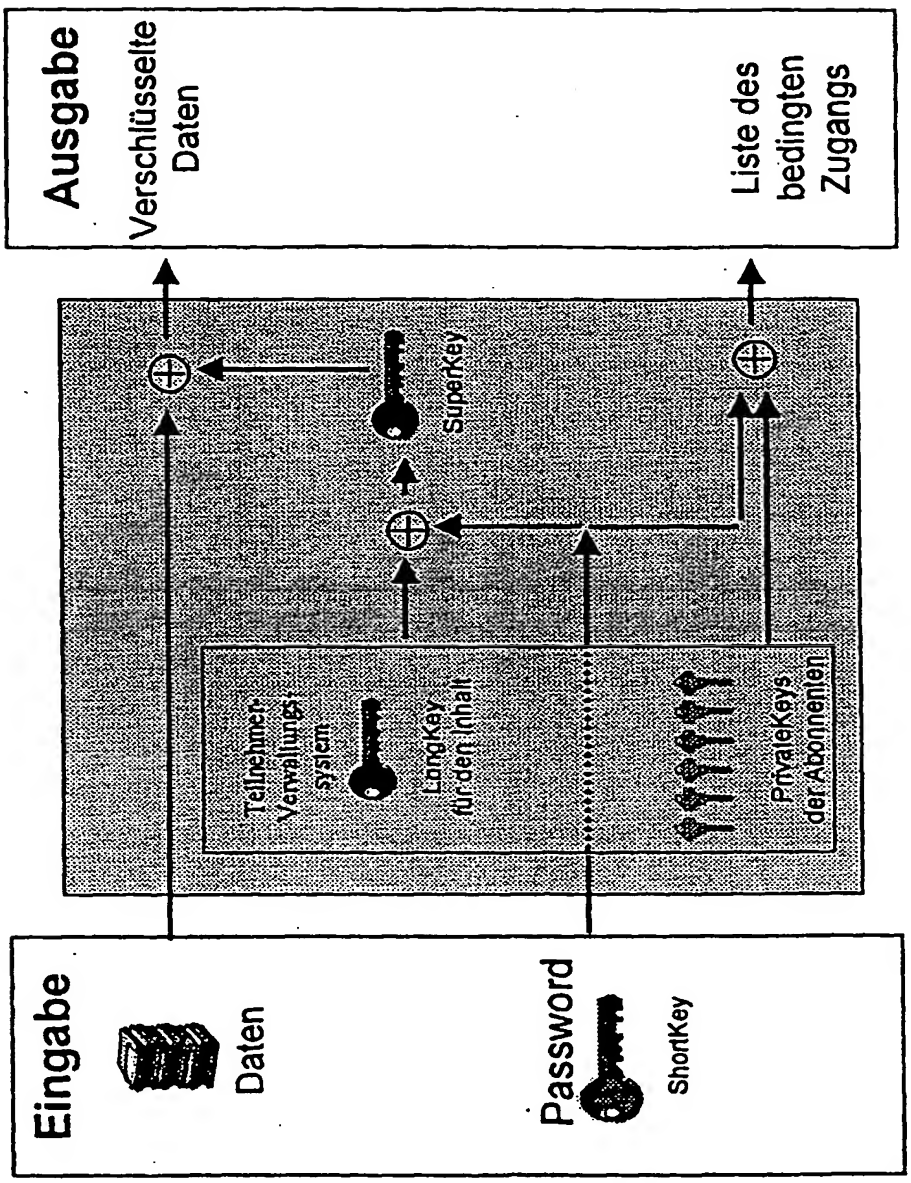
Ausgabe
Verschlüsselte Daten
Liste des bedingten Zugangs
SuperKey
Teilnehmer-Verwaltungs-system
LongKey für den Inhalt
PrivateKeys der Abonnenten
Eingabe
Daten
Password
ShortKey

Fig. 1

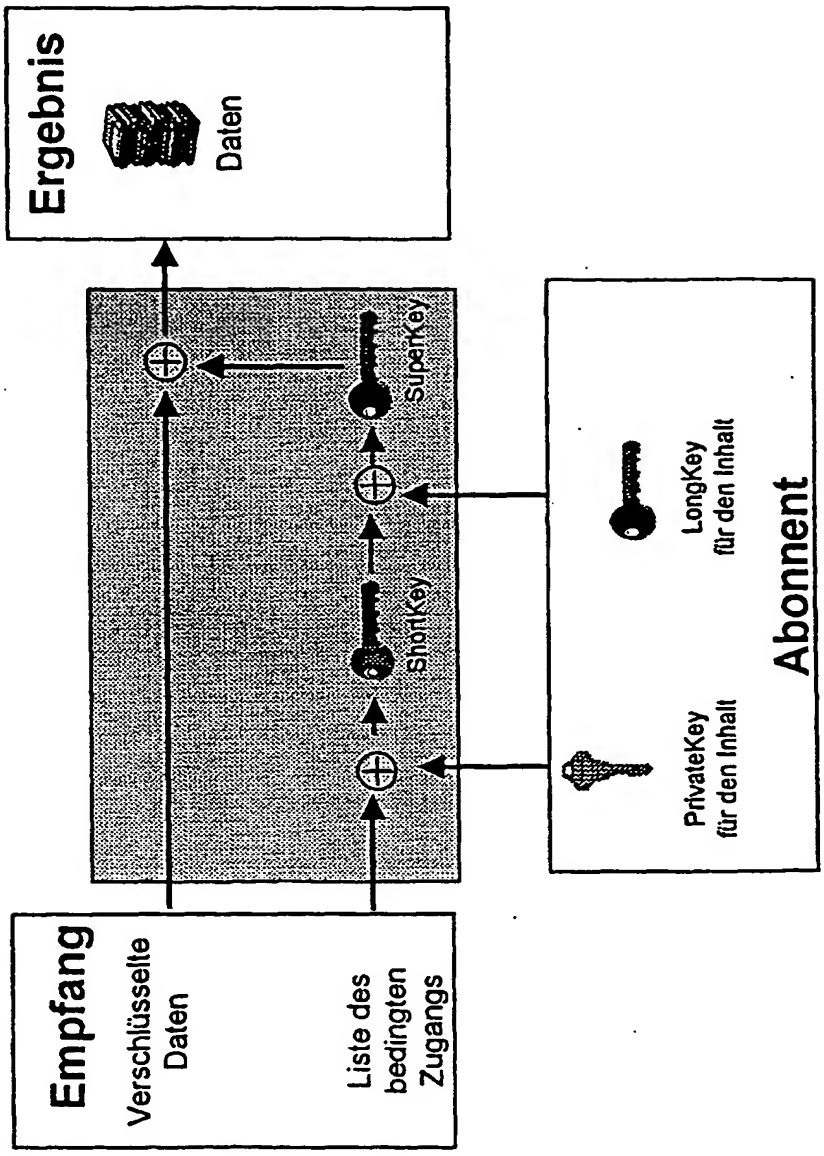
Ergebnis
Daten
SuperKey
ShortKey
LongKey
für den Inhalt
PrivateKey
für den Inhalt
Abonnent
Empfang
Verschlüsselte
Daten
Liste des
bedingten
Zugangs

Fig. 2

Beschreibung der Schlüssel

PrivateKey: **Typ: Statisch** **Besitzer: Inhaltsanbieter & Abonnent**

Für jeden Content-Abonnenten wird ein individueller PrivateKey aus den Anmeldungsdaten berechnet. Die Freischaltung erfolgt über diesen Schlüssel.

LongKey: **Typ: Statisch** **Besitzer: Inhaltsanbieter & Abonnent**

Für jeden Content wird ein LongKey bestimmt.

ShortKey: **Typ: Variabel** **Besitzer: Inhaltsanbieter**

Entspricht dem Password für jede Sendung.

SuperKey: **Typ: Variabel** **Besitzer: Keiner**

Für jede Datensendung wird der SuperKey für die Ver- und Entschlüsselung aus LongKey und ShortKey berechnet.

Fig. 3

EP 1 083 749 A2

EUROPEAN PATENT APPLICATION

Publication Date:
March 14, 2001, Patent Gazette 2001/11
Application No.: **001116072.0**
Application Date: **July 27, 2000**

Int. Cl.7: **H04N 7/16**

Stated Convention Signatories:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Stated Extension Countries
AL LT MV MK RO SI

Priority: **07.09.1999 DE 19943698**

Applicant: **Deutsche Telekom AG**
53113 Bonn (DE)

Inventor:
- **Althoff, Jurgen**
  48429 Rheine (DE)
- **Boehnke, Norbert**
  81825 Munich (DE)

Procedure and device for selective data transfer by means of a wireless transmission system

The well-known procedure for selective data transfer over a public wireless network can be carried out with variably encoded data in the subscriber system, provided only the addressees who are in possession of a current key allotted to them personally, e.g. in the form of an updated valid chip-card are also provided with a personal identification number. A fixed secret code valid for a certain time period runs the risk of unauthorized usage. Moreover any kind of timeframe for the beginning and termination of a subscription at arbitrary time is very restrictive.

The invention solves this time problem by providing a system with a multiplicity of keys, one of which changes from one application to the next. The subscriber data are characterized by a static application-specific key (Longkey), the subscribers are distinguished by a first binary static password (Privatekey), out of which the content supplier extracts a second variable password (Shortkey), allotted to the participant, and in its preparation a third key is derived from the aforesaid keys which is varied incessantly (Superkey) in addition to the aforesaid.

Fields of application of the invention are all kinds of secure data distribution emanating from a content provider through one or a multiplicity of transmitters, addressed to a multiplicity of receivers.

DESCRIPTION

[0001] The invention concerns a procedure characterized in more detail in Claim 1 and a device characterized in more detail in Claim 5. Such procedures and devices are generally known and widely applied and are used e.g. by commercial TV providers for antenna-reception, satellite radio and cable television as well as for pay-television, for broadcasts which can only be received by means of a decoder.

[0002] Public as well as such coded transmissions can also be provided with video-text which contains additional information and can be received by a suitable video-text decoder, which can be provided with a graphic processor for faster access, as published, e.g. by Langenkamp/Löwy "Megatext-IC für Videotext und Grafik" RFE 1994, No. 7, p.18-20.

[0003] German Patent DE 40 33 126 A1 also describes video-text systems which use a telephone line as transmission medium for data transfer. In such systems the information providers accumulate data at an information center and the accumulated information is transmitted to users and/or subscribers upon their request via their terminals. In addition to such direct on-call information transfer there is also a tree-like procedure. While the information center transmits the requested data, the pictures received by the subscriber are reported back to the center, so that in case of an interruption, upon request for resumption of service by pressing the reconnection button the transmission continues from the point reached. The reduction of repetition times thus achieved is essential, since a line transmission is slow because of the small band width, quite as it is in "leafing" through a video-text by means of a television receiver, which causes considerable loss of time to the subscriber and long delays until the desired information is obtained. Such devices also lack archiving or memory capacity.

[0004] These disadvantages can be reduced by using a computer equipped with a receiving device provided with a TV plug-in card with antenna connection and state-of-the-art software as a reproduction medium. A receiver-channel memory may also be included and used for video-text and transmitted data storage.

[0005] Other transmission systems are also known in which data are transferred in another format than video-text such as Intel's INTERCAST, now undergoing trial runs at the ZDF [South-German Television].

[0006] Such means can also be used to realize selective data transmission over a public wireless broadcasting system and/or over the internet for providing subscribers with coded data, which can only be decoded by addressees who possess an up to date key personally given to them. Such a key may be, realized as is commonly done, as a valid chip-card together with a personal identification number (PIN) stored in it, eventually in encoded format, so that the addressee's identity is revealed to the content provider only through the former's secret code.

[0007] The use of such secret code which remains unchanged for a certain space of time is risky, however, both for the content provider and for the addressee since unauthorized use of this code can serve for a central assault on system security. In addition, any kind of time-frame for the beginning as well as for the end of a subscription at an arbitrary time is very restrictive. It is therefore the task of the present invention to avoid the use of a fixed secret key and to configure the procedure and the device so that a subscription may commence and terminate at any arbitrary time.

[0008] The invention solves this problem by the procedural steps listed in Claim 1.

[0009] A device suitable for solving this problem is described in Claim 5.

[0010] Advantageous extensions of the procedure are described in sub-claims 2 to 4.

[0011] An advantageous extension of the device is described is sub-claim 6.

[0012] The invention is described in more detail on the example of an embodiment, according to the attached drawings. These drawings show the following:

Fig. 1 overview of the data-key functions in order to draw up a list allowing limited access to the content provider

Fig. 2 overview of the data-key functions in providing a subscriber with data

Fig. 3 overview of the keys used

[0013] The figures illustrate how data and keys are combined and need no additional explanation. Hence the following text describes in some detail the setting up and the termination of a subscription.

[0014] The content provider will draw up a list of all subscription packages offered, with the associated charges.

[0015] The customer receives a product package and a plug-in card for the reception of data packets, antenna connection, plus a recorded installation software. The software contained in the product package initiates a transmitting station search and stores the channels which are found. The customer is also supported by the software in putting through an application.

[0016] When a customer decides to take a subscription, he is provided with an encoded list of the offered subscription packages together with the updated charges.

[0017] The customer next chooses from the list one or more subscription packages and fills an application form.

In this form the customer provides the necessary data concerning his person, such as:

- Name
- Street
- Town
- Manner of payment
- Bank account, If applicable

[0018] The customer can then send the filled form by mail, e-mail or fax to the content provider.

[0019] When the content provider receives a subscription application, a password (Privatekey) is generated for each subscription, based on the customer data. This password is sent back to the customer together with the corresponding group designation e.g.:

group = TVToday, Password (Privatekey) =
123456789abcd.

[0020] When the customer receives this, he records the password once only next to the corresponding group designation on a form supplied for that purpose. These data are stored and from then on the customer is entitled to receive data of that group. In a kind of letter box, which he controls by means of a task bar, he receives data on the scheduled transmission times at which he should have his computer turned on. The computer can also be put to other uses in the course of such transmission, because the data are directly recorded and stored on the hard disc.

[0021] The received data are first corrected for possible reception errors by a reconstitution of the bit sequence (interleaving) and by means of a self-correction algorithm. The data is next automatically decoded with the help of the stored password (Privatekey).

[0022] After final decompression the data are stored on the hard disc at the user's disposal.

[0023] When a subscription application is accepted, a password generator creates an individual customer password (Privatekey), based on the customer's personal data, which is sent back to the customer. When the user receives this Privatekey and enters it in the software he is ready to receive.

[0024] The Privatekey, which the user receives from the content provider, is calculated from the personal data (name and address) of the user. In addition, the index value of the Shortkey list (uncoded file) can also be calculated from the Privatekey.

[0025] Each data packet is encoded before transmission (Superkey). For each encoded data packet an additional file (uncoded file) is generated, containing data needed for the decoding. The uncoded file is received by the customer only who

is authorized to receive data of the corresponding group. Change of the uncoded file does not increase the quantity of data in consequence of the coding.

[0026] The finished data packet, which contains the associated uncoded file, is transmitted by the content provider to a TV transmitting station. From there the data can be transmitted at the scheduled times. The data transmission itself is preceded by a clock-page providing data on the time of the end of transmission.

[0027] Should the user change his reception authorization, e.g. because he is in arrears with the payment of fees, then an invalid Shortkey will be generated for him. With this invalid Shortkey, which the customer software extracts from the Shortkey list, the customer is no longer in a position to set up the valid Superkey without which it is impossible to decode the received data.

[0028] When a subscription is finally cancelled, the corresponding index position on the Shortkey list may be newly assigned.

[0029] Using the described procedure it is possible to carry out secure data distribution from one transmitter to many receivers with the following characteristics:

- Addressing an arbitrary number of users or user-groups;
- Time-variable addressing validity;
- Avoidance of hardware-based identification;
- Variable degree of coding;
- Possibility of key change for each transmission;
- Scaleable degree of coding for each transmission.

List of keys used

Superkey

[0030] The actual data transmission is coded by means of the Superkey. Without the valid Superkey it is impossible to decode the data. The Superkey is worked out from the Longkey and the Shortkey.

Longkey

[0031] The Longkey is the static part of the Superkey. For each group a Longkey is just once determined. The Longkey is transmitted together with the clock-page.

Shortkey

[0032] A Shortkey is generated at the center for each user, from which an indexed list is derived. This list (uncoded file) is transmitted before the transmission of the actual data. What Shortkey is assigned to which user is determined from the index. This index can be worked out from the Privatekey of the customer.

[0033] After submitting his application, the user obtains from the provider a Privatekey.
The Privatekey is worked out from the personal data (name and address) of the user. In addition, the index value of the Shortkey list (uncoded file) may be worked out form the Privatekey.

Claims

1. Procedure for selective data transfer of a wireless transmission system, whereby the data thus distributed are provided by the content provider with additional coded data which may only be decoded by those addressees who are in possession of a valid key personally assigned to them, **characterized in that,**

- the application-specific static data key (Longkey) characterizes the contents, transmission time and address data, and separately, in a subscriber management system, coded passwords which are assigned for authorized access;

- a subscriber management system generates from subscriber personal data a first binary static key-word (Privatekey);

- a second variable key-word (Shortkey) is derived from an assignment list sent in coded form by the content provider which after decoding by means of the Privatekey serves to set up the authorization key, while the data which contain an application-specific key are provided with a third variable key (Superkey) calculated from the said application-specific keys in the course of data preparation, and that

- on the receiving side, all received data are taken in in an address-selective manner using the subscriber personal data and the Superkey extracted and tested for access authorization, and only then decoded, corrected and stored.

2. Procedure according to Claim 1, characterized in that the data are transmitted by the TV station in parallel to the video-text.

3. Procedure according to Claim 1, characterized in that the content provider sends over in addition an uncoded list of currently available subscription packages with the associated purchase conditions.

4. Procedure according to Claim 1, characterized in that the content provider generates an invalid Shortkey in order to terminate a subscription, said Shortkey being extracted from the list of access authorized persons.

5. Device for selective data transfer over a wireless transmission system, whereby the content provider sends data packets to a broadcaster while the receiver is equipped with a computer with a wireless data receiver and a receiving channel memory as well as an antenna connection, **characterized in that** the broadcast data packets sent by the content provider to the broadcaster are provided with addresses, content-group designations and transmission times, are compressed, coded and provided with a decoding file and that the receiving device is equipped with subscription and password memories and filters, in addition to the receiving channel memory, and is provided with a switch for connection to a hard-disc area assigned to such subscription activity.

6. Device according to Claim 5, characterized in that the receiving channel memory of transmitted data packets is remotely controlled.

Fig. 1 [on the left:]
Data
Password
Shortkey
[center left:]
Subscriber Management System
Longkey for the contents
Privatekeys of the subscribers
[center right:]
Superkey
[on the right:]
Output
Coded data
Conditional Access List
Fig. 2
[on the left:]
Reception
Coded data
Conditional Access List
[on the right:]
Result
Data
[bottom:]
Privatekey for the contents
Longkey for the contents
Subscriber
Fig. 3
Description of keys

Privatekey:	**Type: Static: Owner: Content Provider and Subscriber** **For each content subscriber an individual private key is worked out from the subscription application data. This key is used to decode the content.**
Longkey:	**Type: Static: Owner: Content Provider and Subscriber** **For each content a Longkey is determined.**
Shortkey:	**Type: Variable; Owner: Content Provider** **Corresponds to the password for each transmission.**
Superkey:	**Type: Variable; Owner: No one** **For each data transmission a Superkey is worked out from the Longkey and the Shortkey for the coding and decoding.**